

# Net2Speech, Inc

## Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008

**Date Filed:** September 19, 2008

**Name of Company Covered by this Certification:** Net2Speech, Inc.

**Form 499 Filer ID:** 826219

**Name of Signatory:** Kamran Siddiqui

**Title of Signatory:** President

I, Kamran Siddiqui, certify that I am President of Net2Speech, Inc. ("Net2Speech"). I attest that, as an officer of Net2Speech, I am authorized to execute this CPNI Compliance Certification on the company's behalf.

I have personal knowledge that Net2Speech' business methods and the procedures adopted and employed by Net2Speech are adequate to ensure compliance with section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996 ("the Act"), and the Federal Communications Commission's regulations implementing section 222 of the Act, 47 C.F.R. § 64.2005, 64.2007 and 64.2009.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year. The company has no information to report with respect to the processes pretexters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: Kamran Siddiqui  
Kamran Siddiqui  
President

## **Accompanying Statement to Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008**

to the extent Net2Speech receives or obtains access to CPNI, it has implemented the following practices and procedures with respect to the use, marketing, and disclosure of such CPNI:

### Employee Training and Discipline

- Train all employees and personnel as to when they are and are not authorized to use CPNI.
- Institute an express disciplinary process for unauthorized use of CPNI.

### Sales and Marketing Campaign Approval

- Guarantee that all sales and marketing campaigns are approved by management.

### Record-Keeping Requirements

- Establish a system to maintain a record of all sales and marketing campaigns that use their customers' CPNI, including marketing campaigns of affiliates and independent contractors.
- Ensure that these records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- Make certain that these records are maintained for a minimum of one (1) year.

### Establishment of a Supervisory Review Process

- Establish a supervisory review process for all outbound marketing situations.
- Certify that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval.

### Opt-In

- Guarantee that the Company only discloses CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties only after receiving "opt-in" approval from a customer.
- Verify that the Company enters into confidential agreements with joint venture partners, independent contractors or any other third party when releasing CPNI.

### Opt-Out Mechanism Failure

- Establish a protocol through which the Company will provide the FCC with written notice within five (5) business days of any instance where opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

## Compliance Certificates

- Execute a statement, signed by an officer, certifying that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI regulations.
- Execute a statement detailing how operating procedures ensure compliance with CPNI regulations.
- Execute a summary of all customer complaints received in the past year concerning unauthorized release of CPNI.

## Customer Authentication Methods

- Institute customer authentication methods to ensure adequate protection of customers' CPNI. These protections only allow CPNI disclosure in accordance with the following methods:
  - Disclosure of CPNI information in response to a customer providing a pre-established password;
  - Disclosure of requested CPNI to the customer's address or phone number on record; and
  - Access to CPNI if a customer presents a valid photo ID at the carrier's retail location.

## Customer Notification of CPNI Changes

- Establish a system under which a customer is notified of any change to CPNI. This system, at minimum, notifies a customer of CPNI access in the following circumstances:
  - password modification,
  - a response to a carrier-designed back-up means of authentication,
  - online account changes, or
  - address of record change or creation.

## Notification to Law Enforcement and Customers of Unauthorized Access

- Establish a protocol under which the appropriate Law Enforcement Agency ("LEA") is notified of any unauthorized access to a customer's CPNI.
- Ensure that all records of any discovered CPNI breaches are kept for a minimum of two (2) years.